Desvendando as Artimanhas Virtuais: um projeto sobre a tipificação de golpes digitais e a promoção da conscientização popular

Uncovering Virtual Artifices: a project on classifying digital scams and promoting popular awareness

Raquel A. Valério[1], Ana Paula V. Dias[1], Patricia C. de Souza[1], Daniel A. Vecchiato[1], Aurélio M. da Silva[2], Nelcileno V. S. Araújo[1]

[1]Instituto de Computação – UFMT – CEP 78.060-719 – Cuiabá – MT – Brasil

[2]CISC – CEP 78.635-000 – Água Boa – MT – Brasil

rakel_arantes@hotmail.com, apaulavieira927@gmail.com,
aureliomsilva1@gmail.com, (patricia, daniel, nelcileno)@ic.ufmt.br

Abstract. *In recent years, society has experienced significant transformations in communication, leading to the widespread use of technologies for interaction, which culminated in the need for digital links, however, this also increased the occurrence of cyber scams. This article addresses the increase in these crimes and the lack of adequate classifications for them. Using the Design Science Research method, the article proposes an artifact to solve this problem, using quizzes to help raise awareness about digital scam patterns. The results show the positive acceptance of the participants, although they indicate the need for adjustments and development of new artifacts.*

Keywords: digital scams; security; awareness; gamification; DSR.

Resumo. *Nos últimos anos a sociedade experimentou transformações significativas na comunicação, levando ao uso disseminado de tecnologias para interação, que culminou na necessidade dos elos digitais, contudo, isso também ampliou a ocorrência de golpes cibernéticos. Este artigo aborda o aumento destes crimes e a ausência de tipificações adequadas para os mesmos. Através do método Design Science Research (DSR), o artigo propõe um artefato para solucionar essa problemática, utilizando quizzes para auxiliar na conscientização sobre os padrões dos golpes digitais. Os resultados evidenciam a aceitação positiva dos participantes, embora indiquem a necessidade de ajustes e desenvolvimento de novos artefatos.*

Palavras-chave: golpes digitais; segurança; conscientização; gamificação; DSR.

Introdução

Na sociedade moderna, a tecnologia tomou conta da vida das pessoas, na tentativa de construir um ecossistema tecnológico e fomentar práticas híbridas, assim facilitando as atividades do dia a dia. Entretanto, justamente por ter se tornado algo comum, criminosos utilizam dos dispositivos eletrônicos conectados à internet, usados na facilitação da comunicação, para aplicar golpes digitais. De acordo com a Fortinet (2022), o Brasil foi o segundo país da América Latina que mais sofreu ataques cibernéticos. As tecnologias criadas foram aprimoradas com os anos e isso tornou extremamente simples aprender a usar os dispositivos de forma negativa, culminando no surgimento de diversos tipos de crimes digitais, como por exemplo: falsificação de dados financeiros e cartões de crédito, golpes e fraudes aplicados por meio de redes sociais e anúncios falsos.

A disseminação de conhecimento sobre estes crimes e seus padrões é essencial para auxiliar na conscientização da população, a fim de que não caiam nos golpes. Então, a partir dessa perspectiva, este projeto foca em criar formas de chamar a atenção dos usuários para o aprendizado de tais conhecimentos, assim propiciando o ensino lúdico por meio do uso de jogos. Dessa forma, é bom salientar que este é um trabalho inicial, já que o projeto de pesquisa em questão teve seu início recentemente. Por este motivo, os participantes encontram-se nas etapas iniciais de pesquisa e tem como objetivo realizar melhorias e adaptações para garantir a qualidade do trabalho.

Trabalhos e conteúdos relacionados

Partindo da ideia do uso da gamificação para conscientização dos golpes digitais e seus padrões, alguns trabalhos relacionados foram encontrados na literatura para que houvesse embasamento teórico sobre a temática. Ademais, também foram pesquisados trabalhos, artigos e sites relacionados ao tema crimes digitais, a fim de estabelecer uma base maior de conhecimento sobre o assunto.

Marinho e Bodê (2022) descrevem que a gamificação foi muito útil para treinamento e conscientização em segurança da informação. Usando o software Kahoot!, obtiveram uma resposta de 66% na melhora do desempenho dos alunos de graduação da Fatec Americana - Ministro Ralph Biasi.

Boopathy, Sreejith e Bithin (2015) usaram a gamificação para ensinar aos alunos vários conceitos de segurança cibernética, através do jogo CTF (Capture the Flag ou Capture a Bandeira). A metodologia de ensino foi dividida em níveis: primeiro, realizaram o round de aprendizagem, depois o round de perguntas e respostas, e, por fim, o próprio CTF, no qual foram ensinadas técnicas de ataque e defesa de sistemas.

Silva e Vieira (2021) explicita em seu artigo conceitos sobre segurança cibernética e como esse termo é entendido de formas diferentes por outros autores. Além disso, apresenta os impactos dos crimes online e os aspectos jurídicos que envolvem os golpes digitais, como a Lei Carolina Dieckmann (Lei Nº 12.737). Também aborda os crimes cibernéticos mais frequentes no Brasil, destacando a publicidade enganosa como o mais comum.

Metodologia

O foco deste projeto de pesquisa concentra-se na construção de um artefato para resolução da problemática identificada, utilizando o método Design Science Research.

Em Design Science Research [Dresch, Lacerda e Antunes 2015]: fazendo pesquisas científicas rigorosas atreladas ao desenvolvimento de artefatos computacionais projetados para a educação, é demonstrado que o método visa abordar problemas práticos, gerando conhecimento científico por meio da criação de um artefato final. O processo de estudo teórico e elaboração de um possível artefato envolve dois ciclos: O ciclo do design, nele trata-se do artefato como objeto que será projetado para solucionar um problema do mundo real, no contexto do estudo feito. O segundo ciclo é o do conhecimento (ou rigor), onde se elabora aspectos teóricos relacionados ao comportamento humano. Existe uma importante inter-relação entre os dois ciclos, as conjecturas teóricas direcionam o projeto do artefato, e conforme o design desta ideia, são feitas mudanças para melhorar a conjectura teórica. A metodologia pode ser resumida em pontos principais de um processo: identificar o problema e sua motivação; definição de objetivos; projeto e desenvolvimento; demonstração do artefato no contexto escolhido; avaliação e comunicação. Sendo os dois primeiros, parte dos ciclos teóricos da pesquisa.

Desenvolvimento e demonstração

Conforme o método DSR, e após estudo de alguns materiais sobre uso de jogos no ensino e sobre golpes digitais, foi criada uma base de conhecimento que ajudou no desenvolvimento do tema escolhido e na solução de sua problemática. A conscientização da população sobre os padrões de alguns golpes digitais através da gamificação, a qual é de extrema importância para o aprimoramento do ecossistema tecnológico e de incentivo à práticas híbridas seguras.

Foram elaboradas tipificações com o auxílio de um investigador da Delegacia Municipal de Água Boa - Mato Grosso, após o mesmo avaliar Boletins de Ocorrência no período de 01/02/2021 até 23/02/2022. Com base nos registros, identificaram-se 5 tipos de golpes recorrentes: "Empréstimo", "Falsa foto de perfil - WhatsApp", "Intermediário", "Número novo" e "Gatinha(o)", com padrões semelhantes, descritos na Tabela1.

Tabela 1. Tabela de tipificação dos golpes escolhidos para o artefato

Nome do golpe	**Como acontece:**	**Qual o meio eletrônico:**	**Cuidados necessários**
Golpe do empréstimo	Os golpistas utilizam ofertas falsas de crédito fácil e rápido, que parecem muito atrativas. Para obter o empréstimo, a vítima é solicitada a fornecer seus dados pessoais. Além disso, para receber o dinheiro, é exigido que a vítima faça uma transferência de um determinado valor para resgatar o empréstimo.	Opera através de mensagens em aplicativos de conversa, ou SMS, e por meio de anúncios enganosos em redes sociais ou enviados por e-mail.	É importante ficar atento a ofertas tentadoras que parecem suspeitas. Evite concordar em fazer pagamentos parcelados do empréstimo para contas de pessoa física. Não realize transferências bancárias antes de receber o valor acordado. Procure sempre empresas com boa reputação.

Falsa foto de perfil do whatsapp	O golpista finge ser outra pessoa e usa a foto do perfil da vítima. Em seguida, ele envia mensagens aos conhecidos da vítima cujos dados foram roubados, informando que mudou de número e pedindo dinheiro.	As mensagens são encaminhadas por Whatsapp.	Sempre verifique a identidade do contato e ative uma senha ou autenticação em duas etapas no aplicativo de mensagens.
Intermediário	Essa fraude acontece quando alguém intermedeia uma negociação, prometendo lucros financeiros. Porém, existem transações obscuras envolvendo altas quantias de dinheiro. Isso acaba prejudicando a vítima, pois o valor prometido nunca é recebido.	Ocorre principalmente por anúncio em redes sociais.	Os usuários devem manter-se cautelosos em relação a anúncios que prometem lucros elevados de forma fácil. É fundamental verificar a credibilidade de tais negociações financeiras.
Número novo	A vítima recebe uma mensagem no aplicativo WhatsApp, onde o remetente se faz passar por alguém conhecido, mesmo que o número não conste em sua lista de contatos. Logo após, o criminoso pede dinheiro à vítima.	Ocorre por meio de aplicativos de conversa, tais como: Whatsapp e Telegram.	Esta situação explora o lado emocional da vítima, já que o golpista finge ser um amigo ou ente querido em uma situação de extrema urgência. Isso leva a vítima a se comover. Sempre verifique o histórico de contatos e entre em contato com a pessoa pelo número para confirmar sua identidade.
Gatinha	Um perfil fictício de alguém atraente solicita amizade à vítima. O golpista inicia uma conversa, solicitando a troca de fotos íntimas. Posteriormente, o indivíduo que se passa pelo pai da pessoa afirma que se trata de um menor de idade e, para evitar denúncia à polícia, o golpista requer o pagamento de dinheiro.	Este golpe começa nas redes sociais, tais como: Facebook e Instagram, e continua com a troca de fotos pelo WhatsApp durante a conversa com a vítima.	Ao receber um pedido de amizade nas redes sociais, é crucial avaliar se a conta é recente, se contém um número significativo de fotos publicadas, se possui uma extensa rede de conexões e interações, e se esses seguidores são autênticos.

De posse da tipificação dos golpes decidiu-se por desenvolver quizzes, como artefato final do DSR. Foi realizada uma busca abrangente para escolher a plataforma de criação de quizzes, considerando critérios como idioma, gratuidade, compartilhamento, tipos de perguntas, tempo, comentários e pontuação. A plataforma escolhida foi a Quiz Maker, por ser internacional, online e de fácil jogabilidade.

Depois de identificar os padrões de crimes digitais, foram formuladas 25 perguntas, distribuídas em conjuntos de 5 para cada tipo de golpe, em conjunto com o investigador da polícia. Esses questionários foram divulgados semanalmente nas redes sociais e entre contatos pessoais, com o intuito de disponibilizar todos em um prazo máximo de 2 meses e impulsionar o aumento de seguidores no perfil do projeto no Instagram. Os links diretos para os questionários foram disponibilizados para acesso facilitado.

Para avaliação dos quizzes como artefato final de pesquisa, foram criados formulários do Google para cada um. O perfil dos usuários era de 19 a 35 anos, com pontuação média de 8/10, indicando bom conhecimento sobre golpes. Alguns jogadores tiveram dificuldades com a formulação e ramificação das perguntas.

Considerações finais

Após análises, verificou-se que os quizzes foram eficazes na sensibilização acerca dos golpes digitais, porém demandam ajustes. Para abordar essa questão, será implementada uma nova estratégia que envolve a revisão dos quizzes existentes e a criação de novos recursos. Além disso, está prevista a elaboração de uma plataforma dedicada ao conhecimento científico. O estudo sobre golpes digitais prosseguirá para garantir a atualização contínua do conteúdo.

Agradecimentos

Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, a Universidade Federal de Mato Grosso - UFMT e o Instituto de Computação - IC.

Referências

Boopathy, K., Sreejith, S. e Bithin, A. (2015). Learning cyber security through gamification. In *Indian Journal of Science and Technology*, v. 8, n. 7, p. 642-649.

Fortinet (2022) “Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina”,https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a.

Dresch, A., Lacerda, D. P. e Antunes Jr., J. A. V. (2015), Design Science Research: método de pesquisa para avanço da ciência e tecnologia, Bookman.

Marinho, A. e Bodê, J. (2022). Gamificação Aplicada a Programas e Campanhas de Conscientização de Segurança da Informação. In *FatecSeg - Congresso De Segurança Da Informação*.

Silva, R. L. e Vieira, A. (2021). Segurança cibernética: o cenário dos crimes virtuais no Brasil. In *Revista Científica Multidisciplinar Núcleo do Conhecimento*. Ano 06, Ed. 04, Vol. 07, pp. 134-149.